Lecture 6: Equivalence Relations and Partitions
Modular arithmetic.

First, some set theory: If \( X \) is a set, \( X \times X \) is the set of
ordered pairs of elements of \( X \):
\[
X \times X = \{ (a, b) \mid a \in X, b \in X \}.
\]

A relation \( R \) on \( X \) is a subset of \( X \times X \): \( R \subseteq X \times X \)
For \( a, b \in X \), we write \( a \sim b \) to mean \((a, b) \in R \).

NB: We may also use another symbol for the relation,
depending on context.

Ex. "\( a \sim b \)" corresponds to \( R = \{ (x, x) \mid x \in X \} \subseteq X \times X \)
"\( a \sim b \)" \( (a, b \in \mathbb{Z}) \) corresponds to \( R = \{ (a, b) \mid a \sim b \} \subseteq \mathbb{Z} \times \mathbb{Z} \)

Some relations are "like equality".

Def. Let \( R \subseteq X \times X \) be a relation, and write \( a \sim b \) for \((a, b) \in R \).
Then \( \sim \) (or \( R \)) is an equivalence relation if

(i) for all \( a \in X \), \( a \sim a \) (reflexive)
(ii) for all \( a, b \in X \), if \( a \sim b \) then \( b \sim a \) (symmetric)
(iii) for all \( a, b, c \in X \), if \( a \sim b \) and \( b \sim c \), then \( a \sim c \) (transitive)

Def. If \( \sim \) is an equivalence relation on \( X \), the subset of \( X \)
\[
[a] = \{ b \in X \mid a \sim b \} \subseteq X
\]
is called the equivalence class of \( a \).

Observe \( a \in [a] \) since \( a \sim a \) (reflexive property)

Proposition (2.6.5) If \( \sim \) is an equivalence relation on \( X \), then
for \( a, b \in X \), \( a \sim b \) if and only if \([a] = [b]\)
Proof: Suppose \([a]=[b]\). Then \(b \in [b]=[a]\), so \(a \sim b\).

Suppose \(a \sim b\), so \(b \sim a\) by symmetry.

Let \(z \in [a]\) then \(a \sim z\); with \(b \sim a\) and transitivity we get \(b \sim z\), so \(z \in [b]\). It was arbitrary, so \([a] \subseteq [b]\).

Same argument with roles of \(a\) and \(b\) reversed gives \([b] \subseteq [a]\).

So \([a]=[b]\). \(\Box\)

**Corollary (2.6.6)** If \(\sim\) is an equivalence relation on \(X\), \(a, b \in X\),
then either \([a]=[b]\) or \([a] \cap [b] = \emptyset\).

Proof: Must show \([a] \cap [b] \neq \emptyset\) implies \([a]=[b]\). Take \(z \in [a] \cap [b]\)
then \(a \sim z\) and \(b \sim z\). By symmetry and transitivity,
\(a \sim z \sim b\) implies \(a \sim b\). So \([a] = [b]\) by
the proposition above. \(\Box\)

**Def** A partition of \(X\) is a collection \(\mathcal{S}\) of subsets of \(X\)
such that (i) the elements of \(\mathcal{S}\) are pairwise disjoint,
(ii) Every element of \(X\) is an element of some element of \(\mathcal{S}\).

**Example**: \(X = \{1, 2, 3, 4, 5\}\) \(\mathcal{S} = \{\{1, 2, 3, 4, 5\}\}
\) or \(\mathcal{S}' = \{\{1, 2, 3\}, \{4, 5\}\}\)

**Nonexamples** \(\mathcal{S}'' = \{\{1, 2, 3\}, \{4, 5\}\}
\) _these sets overlap!_ \(\mathcal{S}''' = \{\{1, 2\}, \{3, 4, 5\}\}
3\) is not in any of the parts!

**Proposition**: let \(\sim\) be an equivalence relation on \(X\), and define
\(\mathcal{S} = \{[a] | a \in X\}\) to be the set of equivalence classes (with respect to \(\sim\)).
Then \(\mathcal{S}\) is a partition.

Proof: Since \(a \in [a]\), every element of \(X\) is in some element of \(\mathcal{S}\).

Corollary 2.6.6 guarantees that if \([a]\) and \([b]\) are distinct,
they are disjoint. \(\square\)
Conversely, every partition comes from an equivalence relation this way: Given \( S_0 \), declare \( a \sim b \) if \( a \) and \( b \) belong to the same element of \( S_0 \). See Goodman 2.6 for more detail.

**Modular arithmetic.** We now introduce a key equivalence relation on the set \( X = \mathbb{Z} \).

**Def** Fix \( n \in \mathbb{Z}, n \neq 0 \). For \( a, b \in \mathbb{Z} \), we say 
\( a \) is congruent to \( b \) modulo \( n \), written \( a \equiv b \pmod{n} \)

If \( b - a \) is divisible by \( n \): \( n \mid (b-a) \).

**Example** We count "time of day" modulo 12 hours. "A stopped clock is right twice a day." Could also be thought of as modulo 24 hours if we include AM/PM information.

**Proposition** For fixed \( n \), congruence modulo \( n \) is an equivalence relation.

**Proof:**

- **Reflexivity:** Need \( a \equiv a \pmod{n} \) or \( n \mid (a-a) \), i.e., \( n \mid 0 \).
  But \( n \mid 0 \) is true because \( 0 = 0 \cdot n \).

- **Symmetry:** Need \( a \equiv b \pmod{n} \) implies \( b \equiv a \pmod{n} \)
  that is, \( n \mid (b-a) \) implies \( n \mid (a-b) \). This is true because \( a-b \) is the negative of \( b-a \).

- **Transitivity:** Need \( a \equiv b \pmod{n} \) and \( b \equiv c \pmod{n} \) imply \( a \equiv c \pmod{n} \)
  If \( n \mid (b-a) \) and \( n \mid (c-b) \), then \( n \mid [(b-a)+(c-b)] \)
  and \( (b-a)+(c-b) = c-a \), so \( n \mid c-a \), and we are done.

The equivalence classes of this relation are called "congruence classes modulo \( n \)" or "residue classes modulo \( n \)".

**Ex** modulo \( n = 2 \), there are two congruence classes.

\[ [0] = \{ \ldots, -4, -2, 0, 2, 4, 6, 8, \ldots \} = \text{even integers} \]

\[ [1] = \{ \ldots, -5, -3, 1, 3, 5, 7, 9, \ldots \} = \text{odd integers} \]

Observe: \([2] \equiv [0] \pmod{2}\) because \(0 \equiv 2 \pmod{2}\)
Ex. Modulo $n=3$, there are 3 equivalence classes

$[0] = \{ \ldots, -3, 0, 3, 6, 9, \ldots \}$ = integers divisible by 3
$[1] = \{ \ldots, -2, 1, 4, 7, 10, \ldots \}$ = two "kinds" of integers not divisible by 3.
$[2] = \{ \ldots, -1, 2, 5, 8, 11, \ldots \}$

We can get a better understanding of the congruence classes by using remainders:

**Notation:** Given $a$ and $n \geq 1$, denote $\text{rem}_n(a)$ the remainder of $a$ divided by $n$. So $\text{rem}_n(a)$ is defined by the properties $a = qn + \text{rem}_n(a)$ (for some $q$) and $0 \leq \text{rem}_n(a) < n$.

**Remark:** Many programming languages use "a $\%$ n" for $\text{rem}_n(a)$. (This notation has nothing to do with percentages.)

**Proposition** For any $a$, $a \equiv \text{rem}_n(a) \pmod{n}$.

**Proof** By definition, $a = qn + \text{rem}_n(a)$ for some $q \in \mathbb{Z}$.
So $n | (a - \text{rem}_n(a))$, and $a \equiv \text{rem}_n(a) \pmod{n}$.

**Proposition** $a \equiv b \pmod{n}$ if and only if $\text{rem}_n(a) = \text{rem}_n(b)$.

**Proof** If $\text{rem}_n(a) = \text{rem}_n(b)$, then by previous proposition.

$a \equiv \text{rem}_n(a) \equiv \text{rem}_n(b) \equiv b \pmod{n}$

So $a \equiv b \pmod{n}$. (by transitivity)

Conversely, if $a \equiv b \pmod{n}$, then

$\text{rem}_n(a) = a \equiv b \equiv \text{rem}_n(b) \pmod{n}$, so $\text{rem}_n(a) = \text{rem}_n(b) \pmod{n}$

Thus $n | (\text{rem}_n(b) - \text{rem}_n(a))$. But since $\text{rem}_n(a)$ and $\text{rem}_n(b)$ are both nonnegative and less than $n$, we have

$-n < \text{rem}_n(b) - \text{rem}_n(a) < n$, and the only number in this range divisible by $n$ is 0. So $\text{rem}_n(b) - \text{rem}_n(a) = 0$.

**Corollary** There are $n$ congruence classes modulo $n$:

$[0], [1], [2], \ldots, [n-2], [n-1], \text{ and } [r] = \{qn + r \mid q \in \mathbb{Z}\}$.